EXHIBIT 3

FORENSIC DUPLICATION AND ANALYSIS USING ENCASE

This lecture is neither a substitute for licensed training nor a shorted version of the User Manual, but instead an overview of the workings and features of EnCase, a commercial software product made by Guidance Software, Inc. out of Pasadena, CA. It is probably safe to say EnCase is a leading product in the law enforcement community, although in some circles, Maresware and Forensic Toolkit by AccessData Corporation are more popular. Since 1998, Encase has helped with thousands of computer crime investigations, and currently is in its third version (EnCase for Windows 3.0). The software design and operating procedures are a lesson in how criminal justice software should be made and used. It should be noted that this particular lecture note may or may not be up to date with the latest version of the software and its capabilities since software companies are always coming out with new versions and new features. With that in mind, let's examine some of what you'll likely encounter.

EnCase will not run without either a USB or parallel port dongle attached. A dongle is a plastic-encased, thumb-sized EPROM chip, which affords perhaps the best measure of copyright protection. Guidance Software originally used dongle devices and drivers from Rainbow Technologies but have mostly phased those out (during 2005) in favor of security dongles from Aladdin Knowledge Systems (www.aladdin.com) and the second edition (HASP HL) of their dongle at that. Anyone with hopes of trying to obtain a pirated or bootleg copy of Encase is likely to be very frustrated unless they have a dongle. [*Footnote*: It should be mentioned here that law enforcement agencies ought to stay away as much as possible from bootleg, pirated, public domain, or "copied" software in any form. Of course, the argument could be made that "starting out" on limited funds necessitates such things, and in some cases, people in some places have put together "good enough" systems "by hand" in such ways. However, the fact remains that this smacks of impropriety and will seriously discredit an investigation if defense counsel finds ANY improprieties in software licensing, copyright, etc.]

EnCase also used to require creation of an EnCase boot disk, which is in DOS. The boot disk is not currently required, but it's a recommended method of acquisition for error checking or balancing of the investigations. This is because Windows will write and taint evidence on files (such as last accessed time and date stamps). Therefore, DOS is used since it does not rewrite to files. The program is not in DOS, but the boot-up procedure is. Using the disk essentially changes system file references from C:\ to A:\. EnCase also has developed a method of acquisition with Linux machines or "Linen" (EnCase for Linux), and the interface is similar to that of EnCase for DOS but of course the process is completely different from EnCase for DOS.

The next piece of equipment you'll need is a parallel-port lap-link (if using a laptop) or cross-over network cable (if using a desktop). On laptops, this is a null-modem connection. The SUBJECT computer is the one being investigated, and the STORAGE computer is the one running EnCase for Windows. The procedure involves booting the subject computer with the EnCase boot disk, and booting your storage computer into Windows. By launching the Encase program and activating the Preview function, you'll see an exact image of the drive down to the sector layer. Because it's a preview function, saving your work at this point is not possible. The purpose of Preview is to establish probable cause or make efficient use of time. PREVIEW has lots of different scanning options.

The cross-over acquisition method is the most popular method, although some people have resorted to additional hardware write blocking devices, such as EnCase's FastBloc Field Edition (FE) or a product called "Tableau" available from www.forensic-computers.com. Encase is

developing a software write block capability as well as other modules; e.g., (1) the Virtual File System (VFS) which could mount an evidence file as a virtual share folder on your drive, or allow others to connect to it depending on license; (2) the Encryption Decryption Suite (EDS) which would decrypt Windows encrypted files and folders; and (3) the Physical Disk Emulator (PDE) which would allow mounting of the evidence files as physical disks in your system, which can then be used in conjunction with different software. For more information about available modules, one should visit Guidance Software's website.

To ACQUIRE, or image, a hard drive after you found incriminating evidence, the acquire function is used. There are several ways to do this. If you have created a forensic workstation with a hot swappable drive bay, you can simply remove the subject HD and place it in your drive bay, letting it share your IDE ribbon cable. This method requires booting from DOS. Another method is to leave the two computers connected, boot the subject PC from DOS, and at the A:\> prompt, type EN /S, which puts the computer in server mode. Your storage computer launches Encase for Windows, and then you hit the Acquire button. A third method involves network connectivity via a 10/100-BaseT cross-over cable. It doesn't work over a LAN, WAN, or the internet, and you must add the appropriate network card drivers to your DOS disk. Mac and Unix machines have to be acquired with the first method.

RAID: Redundant Array of Inexpensive Disks

Many suspects have large hard drive storage needs, so they set up a RAID array of multiple hard drives on their computer. There is a hardware and software way to do this. The hardware method involves buying a RAID controller, and setting up a series of hard drives to be seen by the BIOS as one hard drive. The software method uses the OS, not the BIOS, to create the RAID. With the hardware configuration, EnCase acquires the RAID as if it were one single drive. With the software configuration, each drive is acquired individually.

After acquisition, important steps to take are write-blocking the evidence file, password-protecting it, and changing the evidence file's compression. These steps protect the investigator from charges of tampering, ensure authenticity, and save storage space. Using compression during acquisition will slow down the acquisition process. The standard size of a compressed evidence file is 640MB, which is burned on a CD-ROM. Each file acquired will also have an MD5 checksum that is kept in the hash library of Encase.

To ANALYZE the evidence file, you can start working with images or begin by doing text string searches. After each file is viewed, the investigator "bookmarks" it into his or her own filing system, making up their own folder names, like "porno", "forgeries", "break-ins", or "fakeIds." There are additional ways to view the evidence: Gallery (or thumbnail) views for images; Timeline views (for looking at patterns of file creation, editing, last accessed); and Report views (which make a court-admissible record of files viewed).

It is possible to run searches on the evidence and perform signature analysis at the same time. Signature analysis computes if there are any hash value discrepancies between a file's extension and the file's header (what programs created and opened it). This allows recognition of the type of file regardless of the file extension, and makes for interesting analysis of file origins. Searching for text strings is the main way to find digital evidence, however. EnCase supports case-sensitive searches, GREP searches, Unicode searches, and multi-term searches.

Review of the Registry files is important because the investigator wants to find out what programs have been installed, what devices have been loaded, and user information. Win9x systems have one registry file, called system.dat while NT/2000 systems have multiple registry files. Add-in functions allow running scripts to see how different processes found in the Registry execute.

Once evidence has been analyzed, it should be organized into a Final Report, which will consist of bookmarked folder structures, text fragments, documents, and pictures. The investigator might want to consider an additional category for e-mail messages, but it depends upon if they've been read or not. Comments can then be added to each file, such as "This is document on growing psychedelic mushrooms" or "This is a picture of a pre-teen having sex." Reports are customizable, but they essentially contain the following type of information in an enumerated list of all files used in evidence:

1) File Name: teensex001.jpg
Full Path: Toast C Drive\Windows\Temp Internet Files\...
Last Accessed: 05/05/02
Last Written: 01/19/02 03:48:44PM
Logical File Size 12,943
Comment: This is a picture of a pre-teen having sex
Acquisition: EnCase version 3, zero errors
Acquisition Hash: 4CD90348D1C009D78E256
Verfication Hash: 4CD90348D1C009D78E256
Drive Geometry: Total Size 4.8GB (10,002,825 Sectors)
Investigator's Name: Dick Private

INTERNET RESOURCES
Learning by Doing
GIAC Article on Computer Forensics Procedures
Guidance Software, Inc.
NIJ Test Results on Computer Forensic Tools

PRINTED RESOURCES
Keightley, R. (2002). *EnCase version 3.0 User Manual.* Pasadena: Guidance Software.

Last updated: 12/10/05
Syllabus for JUS 426
MegaLinks in Criminal Justice